Remarks/Arguments

Claims 1-50 are pending in this application. Claims 2, 3, 26 and 27 have been cancelled without prejudice. Claims 1, 25, 35 and 40 have been amended, and new claims 42-50 are added in this Amendment. Claims 25, 35 and 40 have been amended to correct typographical or grammatical errors. These corrections do not narrow the scope of the claims, nor are they made for any substantial reason related to patentability. They merely present the claims in clearer form. New claims 42-50 have been added to further point out and claim the subject matter the Applicant regards as his invention.

I. Rejections under 35 USC §112

Claim 8 is rejected under 35 USC §112, second paragraph, as "being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention."

Claim 8, recites "wherein the first time period is about the same duration as the second time period." The term "about" is a term of degree, which is recognized by the MPEP (2173.05(b), as being definite where the specification provides some standard for measuring that degree. The specification recites at least one example of two time periods of substantially the same duration, at paragraph [0083] ("The manufacturer could equally well have 5 variant keys or 100 and might have a policy of changing the keys every month...") (emphasis added). Months are about the same duration, but not exactly the same duration, since months contain anywhere from 28-31 days. Thus, the term "about" is not indefinite.

II. Rejections under 35 USC §102

Claims 1-3, 5, 9, 11-13, 16, 25-27, 29, 33, 35, 37 and 41 are rejected under 35 USC §102, as being anticipated by Erickson (U.S. Patent 6,212,639). Claims 2-3 and 26-27 have been canceled. Claims 1 and 25 have been amended to more distinctly claim the subject matter of the invention.

"[A] claim is anticipated if each and every limitation is found either expressly or inherently in a single prior art reference." Celeritas Techs., Ltd. v. Rockwell Int'l. Corp., 150

F.3d 1354, 1361, 47 U.S.P.Q.2d 1516, 1522 (Fed. Cir. 1998). The standard for lack of novelty, that is, for "anticipation," is one of strict identity. Trintec Indus., Inc. v. Top-U.S.A. Corp., 295 F.3d 1292, 1296, 63 U.S.P.Q.2d 1597, 1600 (Fed. Cir. 2002). In the present Office Action, the Examiner's rejection is based on the Erickson reference, which fails to show all of the elements of the claimed invention.

The Erickson reference is very different from what is claimed in this patent application. Erickson's primary idea is to put the encryption circuitry in the configuration memory (serial EPROM), along with a security initialization circuit in the FPGA. (see Erickson, FIG 1) This allows the FPGA and serial EPROM to implement an active cryptographic protocol to secure the communication of bitstream information across the wire between them. In Erickson's primary embodiment, the security initialization circuit in the FPGA provides a key to the encryption circuit in the configuration memory. (3: 31-32) The security circuit uses this key to encrypt the configuration data stored in the configuration memory (3:32-34), and this encrypted configuration data is then sent to the FPGA. (3:34-36). Once the FPGA receives the encrypted configuration data, the FPGA decrypts the data (3:36-39) and uses it to configure the FPGA. (3:39-42).

The Erickson reference also includes an alternate embodiment where the encryption circuit is provided by external resources such as a computer-aided design (CAD) tool like XACT Step. (4:15-19). In this alternate embodiment, the configuration data is encrypted by the CAD tool, before it is ever stored on the configuration memory. (4:15-19) The FPGA then receives the encrypted configuration data, and decrypts it. (4:24-26) The Erickson reference also teaches combining these two methods to doubly encrypt the configuration data. (4:30-39). The Erickson reference, however, does not teach or suggest providing unencrypted configuration data to the FPGA, and having the FPGA itself perform the encryption of the configuration data. The passage in Erickson recited by the examiner, at col. 5, lines 7-20, discusses a feature where the FPGA periodically creates new keys and sends those new keys to the storage device 120, so the storage device 120 can use the new keys to change how it encrypts the configuration data. This passage has nothing to do with having the FPGA itself perform the encryption of the configuration data.

The invention of amended claim 1 and its dependent claims, by contrast, recites "loading an unencrypted bitstream into one of the first plurality of FPGA integrated circuits to generate a secure bitstream using the first secret key" and the invention of amended claim 25 and its dependent claims recites "loading an unencrypted bitstream into one of the first plurality of programmable integrated circuits to generate a secure bitstream using the first secret key. Thus these claimed inventions both recite "loading an unencrypted bitstream" and using the FPGA "to generate a secure bitstream," limitations not taught or suggested by the Erickson reference.

Claims 5, 9, 29 and 33 are similarly not anticipated by the Erickson reference. Claims 5 and 9 depend from claim 1, and claims 29 and 33 depend from claim 25. Since the independent claims 1 and 25 are not anticipated by Erickson, as discussed above, neither are these dependent claims. Furthermore, as noted above, the passage in Erickson recited by the Examiner, col. 5, lines 7-20, relate to the FPGA periodically changing the key it supplies to the storage device. The keys recited in this passage are dynamically created by a security initialization circuit 114. Claims 5, 9, 29 and 33 each relate to keys that are statically fabricated when the integrated circuit (such as an FPGA) is itself created. Once fabricated into the integrated circuit, the keys of claims 5, 9, 29, and 33 are not changeable, whereas the keys generated dynamically by the security initialization circuit 114 are changeable. Thus the Erickson reference fails to teach or suggest the additional limitations of claims 5, 9,29 and 33.

Claims 11 and 35 are similarly not anticipated by the Erickson reference. Claim 11 depends from claim 1, and claim 35 depends from claim 25. Since the independent claims 1 and 25 are not anticipated by Erickson, as discussed above, neither are these dependent claims. Furthermore, neither the cited passages in Erickson nor any other portion of the Erickson reference teaches or suggests the claimed limitation of "wherein there are random differences between artwork" implemented by the masks used to fabricate the two pluralities of integrated circuits claimed, in addition to the different embedded secret keys in each plurality. At best, the Erickson reference teaches that the keys can be stored in "mask programmed circuits." Erickson does not teach the additional limitation of providing additional random differences between the artwork of the two pluralities of integrated circuits. This additional limitation is useful to further disguise the key information in the FPGA, and to inhibit a pirate's efforts to learn where the key

information is stored merely by comparing the two integrated circuits to each other to identify the differences (caused by the different keys) between them.

Claims 13 and 37 are similarly not anticipated by the Erickson reference. Claim 13 depends from claim 1, and claim 37 depends from claim 25. Since the independent claims 1 and 25 are not anticipated by Erickson, as discussed above, neither are these dependent claims. Furthermore, neither the cited passages in Erickson nor any other portion of the Erickson reference teaches or suggests the claimed limitation of "wherein the first secret key is embedded by setting an initial state of a selection of memory cells in a device configuration memory" stored in the integrated circuit (such as an FPGA). The passage of the Erickson reference cited by the Examiner is discussing the initialization of the encryption circuit 125. This encryption circuit is contained in the storage device 120, not in the integrated circuit (i.e. PLD 110). Furthermore, this encryption circuit is not "device configuration memory" as claimed, nor is it a memory of any kind; it is a circuit dedicated to encrypting data.

Claim 16 is similarly not anticipated by the Erickson reference. Claim 16 depends from claim 1. Since the independent claim 1 is not anticipated by Erickson, as discussed above, neither is this dependent claim. Furthermore, as discussed above, the Erickson reference does not teach "loading an unencrypted bitstream into one of the first plurality of FPGA integrated circuits" as claimed. Erickson teaches encrypting the configuration data prior to loading it into the FPGA.

Claim 41 is similarly not anticipated by the Erickson reference. Claim 41 depends from claim 25. Since the independent claim 25 is not anticipated by Erickson, as discussed above, neither is this dependent claim. Furthermore, the Erickson reference does not teach "downloading a secure programmable integrated circuit bitstream through a network" as claimed. The cited passage in the Erickson reference is discussing a "daisy-chain" approach to configuring multiple PLD's on the same circuit board, using a direct wire connection. (9:44-45; FIG. 4) The "secure communications link" referred to by the Erickson reference is not a "network" as claimed, rather it is a conventional "bus" or "daisy-chain" connection between a configuration memory and a number of PLDs on the same board. (9:51-10:2).

Therefore, claims 1-3, 5, 9, 11-13, 16, 25-27, 29, 33, 35, 37 and 41 are not anticipated by the Erickson reference. The applicant respectfully requests that the rejections of these claims be withdrawn.

III. Rejections under 35 USC §103

Claims 4, 7, 8, 18-21 and 31-32 are rejected under 35 USC § 103 as being unpatentable over Erickson.

Case law makes clear that "the best defense against hindsight-based obviousness analysis is the rigorous application of the requirement for a showing of a teaching or motivation to combine the prior art references." Ecolochem, Inc. v. Southern California Edison Co., 227 F.3d 1361, 1371, 56 U.S.P.Q.2d 1065, 1073 (Fed. Cir. 2000). The absence of a convincing discussion of the specific sources of the motivation to combine the prior art references is a critical omission in the Examiner's obviousness analysis, which mainly discusses the way that the Erickson reference can be combined with the other cited references, or unspecific general knowledge to read on the claimed invention.

Combining prior art references without evidence of such a suggestion, teaching, or motivation simply takes the inventor's disclosure as a blueprint for piecing together the prior art to defeat patentability, the essence of improper hindsight. In re Rouffet, 149 F.3d 1350, 1357, 47 U.S.P.Q.2d 1453, 1456 (Fed. Cir. 1998).

A determination of motivation to support an obviousness rejection requires a factual finding that a skilled artisan has knowledge of the principle of the invention. To render a claim obvious "the reasons why one of ordinary skill in the art would have been motivated to select the references and to combine them to render the claimed invention obvious" must be identified specifically. In re Rouffet, 149 F.3d 1350, 1359, 47 U.S.P.Q.2d 1453, 1459 (Fed. Cir. 1998). In the present Office Action, the Examiner's rejection is based on the Erickson reference in view of the other cited references or the unspecific general knowledge, which fails to show the motivation for combining elements of the instant invention.

Claims 18-21 and 31-32 are not obvious in light of the Erickson reference, because they depend from independent claims that are neither anticipated by nor obvious in light of the Erickson reference. Claims 4, 7 and 8 depend from claim 1, and claims 31-32 depend from

claim 25. Since the independent claims 1 and 25 are not anticipated by Erickson, as discussed above, neither are these dependent claims. Furthermore, the Examiner has not cited to any prior art reference which in combination with Erickson would teach all of the limitations of claims 4, 7, 8, 18-21 or 31-32. Thus it appears that the Examiner is relying merely upon some sort of vague, unspecific general knowledge. Neither the Erickson reference nor this unspecified general knowledge provide any motivation to combine Erickson with the general knowledge, to reach the claimed inventions. Thus the Examiner's obviousness rejections comprise an improper hindsight analysis.

Claims 4 and 28 are not obvious over Erickson and the unspecified general knowledge. Claims 4 and 28 claim the concept of allocating FPGAs to different geographic areas, and assigning a different key to each reason. This allocation scheme makes it difficult for someone residing in the second geographic area who pirates a particular bitstream (i.e. configuration data) designed for use in the first geographic area to obtain FPGAs which will run the pirated bitstream. Thus the designer of the bitstream can limit the spread of useful pirated copies, by making bitstreams encrypted with the first key (only available in the first geographic area), and not the second key (available in the second geographic area). Erickson, by contrast, teaches the entirely different concept that a PLD 110 and a storage device 120 on the same circuit board can communicate with each other across a wire, using a public key system. (5:20-39). The Erickson reference does not teach nor even suggest the claimed method of allocating FPGAs with different keys to different geographic areas, and there is no motivation to combine Erickson with any other reference, including the unspecific general knowledge cited by the Examiner, to reach the claimed method.

Similarly, claims 7 and 31 claim the concept of allocating FPGAs to different customers, with each customer having FPGAs with a different key. This allocation scheme makes it difficult for a pirate to obtain FPGAs which will run a pirated bitstream belonging to the first customer, because the bitstream will only run on FPGAs having the first key, and those FPGAs are only sold to the first customer, not to the pirate. The Erickson reference does not teach any type of allocation of FPGAs with different keys to different market segments, whether by geographic area or by customer. Furthermore, there is no motivation to combine Erickson with any other reference, including the unspecific general knowledge cited by the Examiner, to reach

the claimed method. The mere fact that the Erickson reference teaches a PLD having a key storage area does not supply any motivation to use that feature in the way claimed in claims 7 and 31. Thus claims 7 and 31 are not obvious over Erickson, even in combination with the unspecific general knowledge.

As to claims 8 and 32, as discussed above, these claims depend from parent claims 5 and 29, which are not anticipated by the Erickson reference, therefore dependent claims 8 and 32 are likewise not anticipated nor rendered obvious by the Erickson reference. The Erickson reference discloses a circuit on the PLD which dynamically changes the key from time to time. By contrast, as discussed above, claims 5 and 29, and therefore dependent claims 8 and 32, claim a static key fabricated into the artwork of the FPGA. Thus claims 8 and 32 are not obvious over the Erickson reference, even in combination with the Examiner's unspecific general knowledge.

Turning to claims 18-21, the Examiner contends that the Erickson reference teaches "storing a second key within an encrypted FPGA bitstream," apparently citing to col. 5, lines 20-57. This cited passage in Erickson teaches the implementation of a public key system to encrypt the data being transferred from the storage device 120 to the PLD 110. This teaching is expressly teaching away from the method claimed in the instant application. In a public key system, there are no keys stored in the encrypted data being transferred. To receive an encrypted data stream, the receiving unit (here the PLD 110) sends its own public key to the sending unit (here the storage device 120). The storage device 120 uses this public key to encrypt the configuration data, and then sends the encrypted configuration data to the PLD 110. No keys are included in this encrypted configuration data. The PLD 110 then uses its private key to decrypt the encrypted configuration data, and loads it into the PLD memory.

In contrast, the method of claims 18-21 claim storing a second key within an encrypted FPGA bitstream, using a first key to decrypt the encrypted FPGA bitstream to recover the second key, and then using the recovered second key to set up a secure network link between the FPGA and a server. An embodiment of these claims is discussed at paragraphs [0148] to [0151]. Thus the Erickson reference does not anticipate nor render obvious claim 18, nor its dependent claims 19-21.

Claims 6, 10, 30 and 34 stand rejected over Erickson in view of Kean (US Patent 6,292,018).

Turning to claims 6 and 30, these claims recite a method where "only one mask differs between the first and second mask sets." The Examiner contends that the Kean reference discloses a method where only one mask differs between a first and a second mask set. The instant application is claiming mask sets used in the manufacturing process for integrated circuits. The mask sets claimed in the instant application are sets of masks used to fabricate integrated circuits, according to standard circuit manufacturing processes. See, e.g. paragraphs [0010]-[0011], [0082]-[0084], [0101]-[0104]. These mask sets are applied to a silicon wafer to imprint a pattern on the wafer that corresponds to the pattern on the masks within the mask set.

The Kean reference has absolutely nothing to do with masks used to fabricate integrated circuits. The Kean reference at column 30, lines 33-60 is discussing a mask register. Mask registers are registers within an active circuit which contain a series of bits that are used to mask out certain bits from an incoming data value, such as a value loaded on the internal data bus 162 of Kean. The masking function performed by the mask registers is a logical data operation wherein a data value is logically AND'ed with a corresponding value in the mask register. This has the effect of eliminating or masking out any data value that corresponds to a corresponding mask value of '0'. There is no relationship between the mask register of Kean and the mask sets of the instant application. Even if the mask register of Kean were combined with the PLD of Erickson, this combination would totally fail to teach a method of fabricating FPGAs "wherein only one mask differs between first and second mask sets." Furthermore, the mask register of Kean is from a totally different field of technology than the mask sets of the instant application, thus there is no motivation to combine these two totally different concepts, even if such a combination would read on claims 6 and 30, which it does not.

Turning to claims 10 and 34, these claims depend from claims 6 and 30, respectively . The Erickson reference, even in combination with the Kean reference, fails to teach the method of parent claims 6 and 30, as discussed above, thus they also fail to teach the methods of claims 10 and 34.

Claims 14-15, 17 and 38 stand rejected over Erickson in view of Plants (US Patent 6,560,743).

Turning to claims 14-15 and 38, these claims recite a method wherein a key is extracted from a larger set of data values by using a CRC algorithm to extract the key. The Examiner

contends that Plants discloses using "a CRC circuit to make sure the correct data is received." The Examiner is correct as to what Plants discloses. However, Plants does not disclose the subject matter of claims 14-15 and 38. Simply put, Plants discloses the conventional use of a CRC circuit to verify the correctness of received data, by comparing a known value included with the data to a signature derived from the data by the CRC circuit. See Plants, (7:58-63). Plants does not use a CRC algorithm to extract a key from a larger set of data values. In the instant application, the CRC algorithm is used for the novel purpose of extracting the key by summarizing the larger set of data values into the smaller key. The extracted key is not compared with anything, nor is it used to verify the correctness of any data. Rather the extracted key is used to encrypt or decrypt data. Thus Plants does not teach the extraction of a key using a CRC algorithm, as claimed in claims 14-15 and 38, and therefore the combination of Erickson and Plants fails to teach or even suggest the inventions of claims 14, 15 and 38. The rejections should therefore be withdrawn.

Turning to claim 17, the Examiner contends that Plants teaches the implementation of a Message Authentication Code (MAC) to check the validity of a data stream in an FPGA, and this in combination with Erickson renders claim 17 obvious. However, as discussed above, Plants teaches the use of a CRC, which is different from a MAC. A CRC does not provide protection against deliberate alteration of the data stream, whereas a MAC does.

A CRC merely provides protection from an accidental alteration of the data stream, for example by a transmission error. The CRC check is run on the data, and if the computed CRC value is different from the CRC value supplied with the data stream, then the data contains an error. However, if someone wants to intentionally alter data, for example to remove a copyright notice, this person merely has to alter the data, compute the new CRC value, and append that new CRC value to the data being transmitted. This intentionally altered data, along with the altered CRC, will not be detected as erroneous, because the CRC check run on the altered data will return the same value as the altered CRC supplied with the data.

With a MAC, however, the person altering the data cannot also make corresponding alterations to the MAC. Unlike a CRC, a MAC is generated using a secret key, such as the key embedded in the FPGA as claimed in claim 17, and applying that key to the data to be protected by the MAC. Thus the MAC is specific to the unaltered data stream, and is tied to the secret key.

If the data is altered, for example intentionally to remove a copyright notice, or unintentionally by a transmission error, then the data will not match the MAC, and the FPGA will reject the data. A pirate wishing to alter the data must also alter the MAC, or else the data will not be accepted by the FPGA. However, altering the MAC requires access to the secret key, which the pirate will not have. Thus, Erickson, even in combination with Plants, fails to teach the use of a MAC as claimed in claim 17, and the rejection should be withdrawn.

Turning to claims 22-24, the Examiner has rejected these claims over Erickson in view of Candelore. The Examiner recognizes that Erickson fails to teach "causing the FPGA to calculate a message authentication code (MAC) corresponding to a user design," and "storing the message authentication code with bitstream information in a nonvolatile memory." The Examiner contends that Candelore teaches "the generation of the MAC and storage device for keeping necessary info to receive the contents data and authentication data (Col 4 lines 45-64)."

Neither the cited passage of Candelore nor any other teaching of Candelore mentions applying any of Candelore's teachings to FPGAs, or to bitstreams for configuring FPGAs, as required by claims 22-24. Candelore discusses using a microprocessor to implement the access control teachings of Candelore, not an FPGA. Thus, Candelore, even in combination with Erickson, does not cause an FPGA to calculate a message authentication code, nor does Candelore store a message authentication code with bitstream information. Furthermore, since the Erickson reference is from the field of FPGAs, and the Candelore reference is unrelated to FPGAs, there is no motivation to combine these two references from unrelated fields. Accordingly, the rejections of claims 22-24 should be withdrawn.

As to claims 23 and 24, the addition of the Kocher reference (US Patent Application Publication 2004/0111631) still does not reach the inventions claimed in claims 23 and 24. First of all, Kocher is a reference about smart-card technology, which is unrelated to FPGA technology. The teachings of Kocher are directed to methods of protecting audiovisual content being broadcast over satellite TV or cable TV networks, such as pay-per-view content. See, e.g., Kocher, paragraph [0038]. Thus there is no motivation to combine the Kocher reference with either the Erickson reference or the Candelore reference.

Furthermore, the Kocher reference contains no details about how the watermarking process is implemented. Kocher merely makes passing remarks that watermarking of "content"

is useable to identify copyright owners. See [0153]. Read in the context of the teachings of Kocher, it is clear that Kocher is discussing protection of audiovisual content being broadcast to consumers, such as pay-per-view television broadcasts. Kocher makes no mention of how to watermark FPGA bitstreams, nor does it even address FPGAs at all. Therefore, even if there were some motivation to combine these references, one skilled in the art would not be able to combine Kocher with Erickson and Candelore to obtain the invention of claims 23 and 24.

The inventions of claims 23 and 24 are directed to storing copyright messages within a bitstream used to configure an FPGA. These methods have nothing to do with the teachings of Candelore (microprocessors) or Kocher (smartcards for cable TV). Accordingly, the inventions of claims 23 and 24 are not obvious over the Erickson, Candelore and Kocher references, and the rejections of claims 23 and 24 should be withdrawn. Similarly, newly presented claims 48-50 are not anticipated nor rendered obvious by any combination of Erickson, Candelore, or Kocher.

IV. Conclusion

Prompt and favorable action on the merits of the claims is earnestly solicited. Should the Examiner have any questions or comments, the undersigned can be reached at (949) 567-6700.

The Commissioner is authorized to charge any fee which may be required in connection with this Amendment to deposit account No. 15-0665.

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

Dated: November 19, 2004

By: Donald Daybell

Donald Daybell
Reg. No. 50,877

Orrick, Herrington & Sutcliffe LLP
4 Park Plaza, Suite 1600
Irvine, CA 92614-2558
Tel. 949-567-6700
Fax: 949-567-6710